COLLABORATIVE MANAGEMENT ENVIRONMENT SECURITY ISSUES

Collaborative Technologies Research Center
Computer Science and Mathematics Division
Oak Ridge National Laboratory

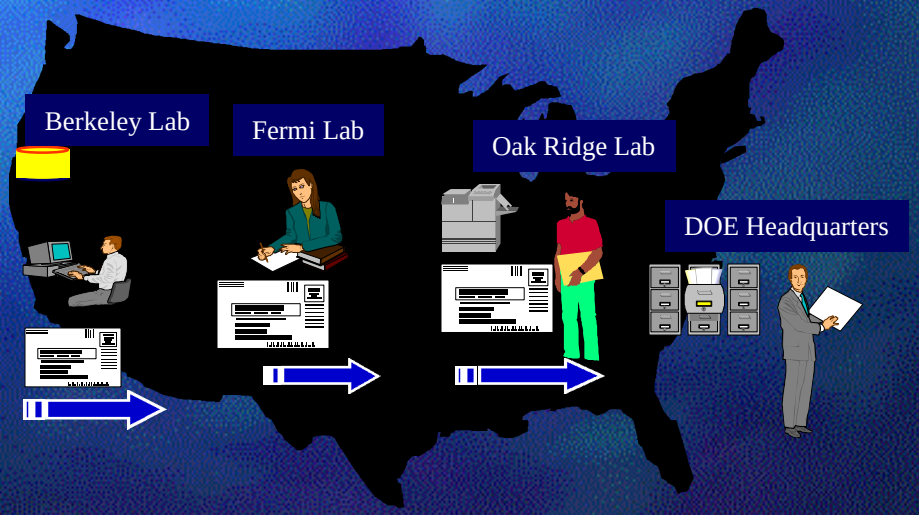
March 18-20, 1998

Presentation Overview

- The CME project is not funded to further security research
- We do have very strong security requirements for our system
- We are interested in using, (not necessarily developing), the security approaches that can address our requirement.

Problem

- Information on thousands of research projects needs to be synthesized for Congressional review
- Data is kept in disparate legacy databases across the country
- The environment is subject to frequent changes
- Transportation of data must be performed in a secure manner



CME Goals and Objectives

- Create an environment to financially manage and analyze research funding
  - Minimal impact to the laboratories
  - Provide complete and consistent data to DOE
- Gain an order of magnitude efficiency in the proposal submission process
- Provide a safe and trusted environment for researchers and program managers

What is a safe and trusted envionment?

- We see the following security requirements for this system
  - Researchers ideas are open to potential sponsors, but closed to competing researchers
  - Program managers have a broad view of research proposals, and a private view of what they fund
  - Lab management has a broad view into work they manage for their labs
  - Unauthorized access to this information must be prohibited

Access Rights

- Multiple people will have access to this data
- Access to information would ideally be based on:
  - The role of the accessor, I.e., a researcher has different access rights than a program manager
  - The scope of responsibility, I.e., a group leader can view the group's work, a lab director can view the entire lab's work.
  - The type or state of information, I.e., a proposal has limited viewing right, and a funded research is generally public information
  - The policy regulating the data, I.e., reorganization changes access rights

Unauthorized Access

- Universally preventing unauthorized access will be difficult
  - Information within the CME system will be distributed and most likely transported over public networks.
  - Data will be stored both remotely and cached locally.
    - a wide number of people will have access to the systems and machines where this information resides
  - Java applets will be used to process and transport data
- Is it feasible to provide universal secure access to this type of data in such an environment?

Are Certificates the Answer?

- Certificates appear to be a sound approach to addressing some of these issues, however:
  - Browser key exchange a major issue
  - Can certificates be easly used for access control?
  - Can Java be trusted with certificates?
  - How much additional processing and cost is required to use certificates?

What about the machines?

- Do we really need to worry about viruses and hackers?
- If so, can we protect ourselves:
  - in a cost effective manor, under $1000 per site?
  - without undue burden, I.e., booting off cards, secure rooms, firewalls,…
- Can we maintain a trusted environment where some participants will be lax with security?

Summary

- CME's goal is to optimize reseach funding
- Several key security issues exist:
  - Controlling access to the data from a variety of factors
  - Preventing unathorized access even in a lax security environment
  - Determining if certificates are the best approach
  - Determining if we can ignore physical machine security issues
- We are open to suggestions and approaches